



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



050.101 Privacy and Security Awareness Program


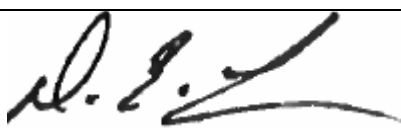
**Version 2.2
May 2, 2018**

050.101 Privacy and Security Awareness Program	Current Version: 2.2
050.000 Security Awareness	Review Date: 05/02/2018

Revision History

Date	Version	Description	Author
11/30/2006	1.0	Effective Date	CHFS OATS Policy Charter Team
5/2/2018	2.2	Revision Date	CHFS OATS Policy Charter Team
5/2/2018	2.2	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS IT Executive (or designee)	5/2/2018	Jennifer L. Harp	
CHFS Chief Security Officer (or designee)	5/2/2018	DENNIS E. LEBER	

050.101 Privacy and Security Awareness Program	Current Version: 2.2
050.000 Security Awareness	Review Date: 05/02/2018

Table of Contents

050.101 PRIVACY AND SECURITY AWARENESS PROGRAM.....	5
1 POLICY OVERVIEW.....	5
1.1 PURPOSE	5
1.2 SCOPE	5
1.3 MANAGEMENT COMMITMENT.....	5
1.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES	5
1.5 COMPLIANCE	6
2 ROLES AND RESPONSIBILITIES	6
2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)	6
2.2 SECURITY/PRIVACY LEAD	6
2.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY OFFICER	6
2.4 CHFS STAFF AND CONTRACTOR EMPLOYEES	7
2.5 TRAINING ADMINISTRATOR	7
3 POLICY REQUIREMENTS	7
3.1 GENERAL	7
3.2 TRAINING CONTENT.....	8
4 POLICY MAINTENANCE RESPONSIBILITY	8
5 POLICY EXCEPTIONS	8
6 POLICY REVIEW CYCLE.....	8
7 POLICY REFERENCES	9

050.101 Privacy and Security Awareness Program	Current Version: 2.2
050.000 Security Awareness	Review Date: 05/02/2018

Policy Definitions

- **Agency:** For the purpose of this document, agency or agencies refers to any department under the Cabinet of CHFS.
- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. SDS Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Insider Threat:** A current or former employee, contractor or business partner who: Has or had authorized access to an organization's network, system, or data and has intentionally exceeded or used that access in a manner that negatively affected the confidentiality, integrity, or availability (CIA) of the organization's information or information systems.
- **Security Awareness Training:** Per the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 guidance, Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

050.101 Privacy and Security Awareness Program	Current Version: 2.2
050.000 Security Awareness	Review Date: 05/02/2018

050.101 Privacy and Security Awareness Program

Category: 050.000 Security Awareness

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a privacy and security program. This document establishes the agency's Privacy and security Awareness Program Policy which helps manage risks and provides guidelines for security best practices regarding privacy and security.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

This policy applies to all CHFS employees and any contractor or other user with a CHFS domain Active Directory (AD) account (hereinafter "contractor"), including all persons providing contractor services, who use, process, or store computerized data relevant to agency business. Any employee, contractor or contracted 3rd party entity with access to CHFS data must participate in or provide a security awareness program. Third parties with access to CHFS data but without a CHFS AD account must manage their own awareness program.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the Cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking exceptions to this policy.

050.101 Privacy and Security Awareness Program	Current Version: 2.2
050.000 Security Awareness	Review Date: 05/02/2018

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This position is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) is designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

050.101 Privacy and Security Awareness Program	Current Version: 2.2
050.000 Security Awareness	Review Date: 05/02/2018

2.4 CHFS Staff and Contractor Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply with referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

2.5 Training Administrator

The training administrator oversees the entire life cycle of the privacy and security awareness training program, this includes annual training initiation, reminders, non-compliant reporting, and escalation to management, as needed.

3 Policy Requirements

3.1 General

This policy defines and details the requirement for privacy and security awareness that data owners are expected to implement to safeguard their computing assets. All new employees and contractors are presented with access to enterprise and cabinet privacy and security policies, standards, procedures, and the CHFS Employee Privacy and Security of Protected Health, Confidentiality, and Sensitive Information Agreement (CHFS 219 Form), prior to the provision of access to any CHFS computing asset. All CHFS employees and contract staff shall be reminded annually of their privacy and security responsibilities. Additionally, the OATS Information Security (IS) Team and the Commonwealth Office of Technology (COT) Security Management Branch is responsible for sending out periodic reminders concerning contemporaneous privacy and security events as well as current privacy and security risks.

To satisfy the requirement for the Privacy and Security Awareness Program, basic privacy and security awareness training to all state and contract staff must be provided:

- Prior to system access;
- When major system change occurs;
- Annually thereafter;

All CHFS agencies will take a standardized training provided by the Information Security Department's training administrator through the Kentucky Online Gateway (KOG). After the training is complete, a multi-question test will be taken and a passing score of 75 percent or higher must be obtained to assure the material was absorbed. Documentation showing completion of training for staff or quiz results must be retained for at least ten (10) years in accordance with the CHFS Records Retention Schedule Kentucky Department for Libraries and Archives (KDLA) requirements.

050.101 Privacy and Security Awareness Program	Current Version: 2.2
050.000 Security Awareness	Review Date: 05/02/2018

3.2 Training Content

The training administrator is responsible for providing the Privacy and Security Awareness Training content to KOG. The training at a minimum shall consist of, but is not limited to the following:

- Security Awareness on recognizing and reporting potential indicators of compromise or insider threats;
- Incident Response procedures or steps;
- Any federal or state laws and regulations that the agency must follow/abide by;
- Explanation of importance and responsibilities the employee has around identifying and protecting sensitive data;
- Employees' responsibilities related to privacy and security in the workplace.

Additional information for the content and requirements for CHFS annual privacy and security awareness training can be found in the CHFS Privacy and Security Awareness Training Procedure.

4 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

5 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

CHFS agencies, such as Child Support Enforcement (CSE), that do not utilize KOG to perform privacy and security awareness training, will be responsible for maintaining documents of proof to ensure privacy and security awareness activities are annually completed.

6 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

050.101 Privacy and Security Awareness Program	Current Version: 2.2
050.000 Security Awareness	Review Date: 05/02/2018

7 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS Confidentiality/Security Agreement/Internet and Electronic Policies and Procedures- CHFS-219 Form
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: CHFS Privacy and Security Awareness Training Procedure
- CHFS Office of Human Resources Management (OHRM) Personnel Procedures Handbook, Chapter II: 2.10
- CHFS Records Retention Schedule Kentucky Department for Libraries and Archives (KDLA)
- Internal Revenue Services (IRS) Publication 1075
- IRS FTI Safeguard Training Certification Acknowledgement Form
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information